Claims 1, 3, 5-17, 19, and 21-23 are pending in this application, with Claims 1, 17, 19, and 22 being independent.

Claims 1, 3, 5-11, 16, 17, 19 and 21-23 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,785,814 (Usami et al.) in view of U.S. Patent No. 6,504,941 (Wong). Claims 12-15 were rejected under Section 103 as being obvious over Usami et al. and Wong when further combined with US 2001/0013097 A1 (Ito et al.). Applicant respectfully traverses these rejections for the reasons discussed below.

As recited in independent Claim 1, the present invention is directed to an image processing apparatus that adds information to image data and encrypts the information-added data. In conventional apparatuses of this type, there is a problem in that someone may be able to discriminate where the added information is located in the image data and tamper with it. Although there may be ways to detect that tampering has occurred, this is not necessarily helpful if the added information has been destroyed. In other words, it is sometimes desirable to prevent tampering with added information, rather than merely detect that such tampering has occurred.

For example, in one embodiment the added information could be tracking information, such as a machine ID number, which allows tracking of which machine was used to generate an image. Thus, if an illegal copy is made, such as counterfeit currency, the machine that is the source of that counterfeit can be traced. In conventional systems, however, if the location of the tracking information is discriminated and that information is tampered with, the added tracking information may be lost. Although the tampering may be detected and the counterfeit recognized as such, it will not be possible to recover the tracking information and identify the source of the counterfeit. Hence, in this situation it

would be preferable to prevent the tampering, so that the tracking information is available to identify the source of the counterfeit, rather than merely to detect that the tampering occurred.

The present invention as recited in independent Claim 1 is directed to addressing this problem and does so by including, *inter alia*, the feature of encrypting information-added data to make it difficult to detect a position where additional information is added to image data, wherein the information-added data is encrypted by randomly arranging the data. This feature is supported, for example, at least in Fig. 9 and the corresponding discussion starting at page 18 of the specification. With this feature of encrypting the information-added data (i.e., the image data to which additional information has been added) by randomly arranging the data, the position where the additional information is added to the image data is difficult to detect and it is more difficult for someone to tamper with the added information. Applicant submits that the cited art fails to disclose or suggest at least the above-mentioned feature. Usami et al. discloses that division means 22 divides an image represented by original image data S0 into areas of a plurality of blocks to obtain image data Sn for each area. Supplementary information generating means 23 generates information regarding photographing as supplementary information H, and optimization means 24 optimizes the supplementary information H for each area divided by the division means 22 to obtain supplementary information Hn for each area. Embedding means 25 then embeds the supplementary information Hn for each area in the image data Sn for the corresponding area using a deep layer encryption to obtain image data S1 containing the embedded supplementary information H. See, Col. 12, ln 17 to col.

13, ln 12. In other words, Usami et al. discloses that the supplementary information Hn is encrypted and the encrypted supplementary information is added to the image data Sn.

Applicant submits that Usami et al. does not disclose or suggest that the information S1 is encrypted after the supplementary information H has been embedded. Therefore, Usami et al. does not disclose or suggest that the *information-added* data is encrypted. Moreover, that patent does not disclose or suggest that information-added data is encrypted to make it difficult to detect a position where the additional information is added, and specifically that patent does not disclose or suggest that information-added data is encrypted by randomly arranging the data. To the contrary, the supplementary information Hn is embedded in the corresponding image data Sn and therefore the position of adding the data is fixed.

The Examiner agrees at page 3 of the Office Action that Usami et al. does not teach the above-mentioned feature, but he asserts that Wong discloses that feature. Applicant respectfully disagrees.

Wong discloses in Figs. 9A and 9B that at least a predetermined block of an image Xr is modified to generate a modified image Xr and a hashed output is calculated from the modified image. A corresponding block of a watermark is combined with the hashed output of the modified image, and then the combined image block is incorporated into the modified image block. This merely discloses that the modified image is hashed before information is added, and then additional information (i.e., a watermark) is combined with the hashed output. Fig. 9A of Wong further shows that public key encryption is performed on the combined data. However, that patent does not show or suggest encrypting information-added data to make it difficult to detect a position where additional

information is added, by randomly arranging the data. In particular, public key encryption involves performing a mathematical operation to modify data using a key; it does not involve randomly arranging the data.

Applicant submits that the disclosure in Wong also does not disclose or suggest randomly arranging the data. The Examiner cites col. 3, lines 10-23 of the specification. However, the discussion at the cited location says nothing whatsoever about encrypting data by randomly arranging the data. Instead, the cited portion merely states that if a watermark is altered (for example, by cropping), then when an extraction procedure is performed it will merely produce an output that resembles random noise, which signifies that the extracted watermark is not valid. Thus, Wong merely discloses an encryption method by which it is possible to detect whether the watermark was tampered with. It does not disclose or suggest encrypting data by randomly arranging the data, which makes it difficult to detect a position where additional information is added to an image, which in turn makes it difficult to tamper with the additional information in the first place.

Accordingly, even if the teachings of Wong were combined with those of Usami et al., Applicant submits that the combination would not disclose or suggest at least the feature recited in Claim 1 of encrypting information-added data to make it difficult to detect a position where additional information is added, wherein the information-added data is encrypted by randomly arranging the data.

Further, Applicant respectfully traverses the Examiner's alleged motivation for combining the teachings of Wong and Usami et al. The Examiner asserts that it would have been obvious to modify Usami et al. in view of Wong because "the confusion of watermark location provides authentication and ownership verification." (Office Action

page 4, citing the abstract of Wong) However, Wong teaches that the authentication and verification functions are performed merely by providing an invisible watermark, and those functions have nothing to do with "confusion of the watermark location." Indeed, as discussed above, Wong merely discloses using public key encryption on combined data and does not teach randomly arranging the data or any other technique relating to confusion of the watermark location.

For the foregoing reasons, Applicant submits that the present invention recited in independent Claim 1 is patentable over the cited art, whether that art is considered individually or in combination. The other independent claims recite similar features and are believed patentable for similar reasons.

The dependent claims are believed patentable for at least the same reasons as the independent claims they depend from, as well as for the additional features they recite.

In view of the foregoing, Applicant submits that this application is in condition for allowance. Favorable reconsideration, withdrawal of the outstanding rejections, and an early Notice of Allowance are respectfully requested.

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 530-1010. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

Attorney for Applicant
Brian L. Klock
Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200
BLK/mls

DC_MAIN 249413v1